



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/607,917	06/26/2003	Kyung-Hun Jang	784-51 (SI-19122-US)	8113
28249 7590 02/21/2007 DILWORTH & BARRESE, LLP 333 EARLE OVINGTON BLVD. SUITE 702 UNIONDALE, NY 11553			EXAMINER HOFFMAN, BRANDON S	
			ART UNIT 2136	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	DELIVERY MODE
3 MONTHS			02/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/607,917	<b>Applicant(s)</b> JANG ET AL.	
	<b>Examiner</b> Brandon S. Hoffman	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 04 December 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-15 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>9-11-06</u> . | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Claims 1-15 are pending in this office action.
2. Applicant's arguments, filed December 4, 2006, have been fully considered but they are not persuasive.

#### ***Information Disclosure Statement***

3. The information disclosure statements (IDS's) submitted on September 11, 2006, and April 27, 2006, are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

#### ***Claim Rejections***

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

#### ***Claim Rejections - 35 USC § 101***

5. Claims 14 and 15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 14 and 15 are not limited to tangible embodiments. In view of applicants' disclosure, specification page 9, line 26 through page 10, line 3, the medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (e.g., ROMs, floppy disks, hard

Art Unit: 2136

disks) and intangible embodiments (e.g., carrier waves). As such, the claim is not limited to statutory subject matter and is therefore non-statutory. Claim 15 is dependent upon claim 14 and therefore inherits its deficiencies.

***Claim Rejections - 35 USC § 102***

6. Claims 1-6 and 8-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Watanabe et al. (U.S. Patent No. 7,072,657).

Regarding claim 1, Watanabe et al. teaches a method for allocating a plurality of encryption keys according to a plurality of access authorization classes, said method comprising the steps of:

- Setting an access authorization to at least one access point in advance (fig. 7, ref. num 502);
- Differentiating said encryption keys according to a plurality of access authorization types (fig. 7, ref. num 510 and 516); and
- Obtaining by at least one wireless station the differentiated encryption keys in advance (col. 7, lines 17-40).

Regarding claims 2, 9, and 13, Watanabe et al. teaches wherein the access authorization types include:

- A class 1 that indicates access authorization to an access point to which the wireless station is assigned;

Art Unit: 2136

- A class 2 that indicates access authorization to predetermined access points included in a local area network (LAN) to which the wireless station is assigned;
- A class 3 that indicates access authorization to all access points included in the LAN to which the wireless station is assigned; and
- A class 4 that indicates access authorization to multiple access points included in a wide area network (WAN) (fig. 4, ref. num 408A-D, 410A-B, and 412A-F).

Regarding claim 3, Watanabe et al. teaches further comprising a step of a wireless station desiring to communicate with an access point selecting from the plurality of encryption keys an encryption key corresponding to the access authorization to the access point and communicates data with the access point, wherein the wireless station has a plurality of encryption keys corresponding to access authorization types (col. 7, lines 17-40).

Regarding claims 4 and 10, Watanabe et al. teaches a method/computer readable medium for allocating one or more encryption keys according to a plurality of access authorization classes, comprising:

- A wireless station requesting an access point to perform authentication and the access point, which is requested to perform authentication, determining access authorization to the access point (fig. 7, ref. num 502);

Art Unit: 2136

- Obtaining an encryption key and generating a shared key set including the obtained encryption keys in accordance with the determination result of the first step (col. 6, line 57 through col. 7, line 16);
- The wireless station requesting a LAN authentication server to perform authentication, and the LAN authentication server, which is requested to perform authentication, determining access authorization to an access point belonging to the LAN (fig. 7, ref. num 510);
- Obtaining an encryption key and updating the shared key set by adding the encryption key to the shared key set in accordance with the determination result of the third step (col. 7, lines 41-64);
- The wireless station requesting a WAN authentication server to perform authentication and the WAN authentication server, which is requested to perform authentication, determining access authorization to an access point belonging to the WAN (fig. 7, ref. num 516); and
- Obtaining an encryption key and updating the shared key set by adding the encryption key to the shared key set in accordance with the determination result of the fifth step (col. 7, lines 41-64).

Regarding claim 5, Watanabe et al. teaches wherein the first step further comprises a step of the wireless station requesting an access point to perform authentication, and the access point which is requested to perform authentication determining whether or not access authorization to the access point corresponds to a

class 1, said class 1 indicating access authorization to an access point to which the wireless station is assigned (col. 7, lines 17-40).

Regarding claim 6, Watanabe et al. teaches wherein the third step of claim 4 further comprises the steps of:

- The LAN authentication server determining whether or not the access authorization to the access point corresponds to a class 2, said class 2 indicating access authorization to predetermined access points included in a LAN to which the wireless station belongs to;
- If a determination result indicates that the access authorization corresponds to said class 2, obtaining an encryption key of class 2, and determining whether or not the access authorization corresponds to a class 3, said class 3 indicating access authorization to all access points included in the LAN to which the wireless station belongs to; and
- If a determination result indicates that the access authorization corresponds to said class 3, obtaining an encryption key of class 3 (fig. 4, ref. num 408A-D, 410A-B, and 412A-F).

Regarding claims 8 and 11, Watanabe et al. teaches a roaming method/computer readable medium for a wireless station using a plurality of encryption keys allocated according to a plurality of access authorization classes, said method comprising the steps of:

- Setting an access authorization to an access point in advance, differentiating said plurality of encryption keys according to a plurality of access authorization types and a wireless station obtaining in advance an encryption key set including the differentiated plurality of encryption keys for respective access points (fig. 7, ref. num 502, 510, and 516 and col. 7, lines 17-40);
- Receiving a command to communicate with an access point not available for communication using an encryption key currently selected in the encryption key set (col. 7, lines 2-4);
- Determining an access authorization to the access point not available for communications (col. 7, lines 4-6);
- Selecting an encryption key from the encryption key set obtained in advance corresponding to the determined access authorization (col. 7, lines 6-9); and
- Using the selected encryption key to encrypt a transmission message and communicate with the access point not available for communication (col. 7, lines 9-16).

Regarding claim 12, Watanabe et al. teaches an apparatus for allocating a plurality of encryption keys according to a plurality of access authorization classes, comprising:

- An access authorization determining unit for determining an access authorization class for communication between a wireless station from a plurality of wireless



Art Unit: 2136

stations and an access point from a plurality of access points (fig. 7, ref. num 400);

- An encryption key storing unit which stores said plurality of encryption keys according to said access authorization classes (col. 6, lines 59-66); and
- An encryption key allocation unit which reads an encryption key from the encryption key storing unit corresponding to a determination result of the access authorization determining unit and transfers a value of said encryption key to the wireless station (col. 7, lines 2-16).

***Claim Rejections - 35 USC § 103***

7. Claim 14, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueda et al. (U.S. Patent No. 6,289,102) in view of Watanabe et al. (USPN '657).

Regarding claim 14, Ueda et al. teaches a computer readable medium **storing instructions which, when executed causes execution of a program implementing** a structure of a wireless data packet used for allocating encryption keys according to access authorization classes in a wireless network that comprises a wireless station and an access point, the **structure** comprising:

- A header of said data packet transmitted through the wireless network (fig. 1, SECTOR HEADER FIELD);
- An encrypted data field in which data contents to be transmitted are encrypted and stored (fig. 1, USER DATA FIELD and fig. 13, section E); and

Art Unit: 2136

- An error correction field, which is used to correct data error (fig. 1, ECC).

Ueda et al. does not teach an access authorization information storing field, which indicates access authorization for communication between the wireless station and the access point.

Watanabe teaches an access authorization information storing field, which indicates access authorization for communication between the wireless station and the access point (fig. 4, ref. num 408A-D, 410A-B, and 412A-F).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a field for access authorization information storing, as taught by Watanabe et al., with the medium of Ueda et al. It would have been obvious for such modifications because the access authorization field tells the device being accessed which level of access needs to take place (see col. 5, lines 50-67 of Watanabe et al.).

Regarding claim 15, Ueda et al. as modified by Watanabe et al. teaches wherein the access authorization types include:

- A class 1 that indicates access authorization to an access point to which the wireless station is assigned;

- A class 2 that indicates access authorization to predetermined access points included in a local area network (LAN) to which the wireless station is assigned;
- A class 3 that indicates access authorization to all access points included in the LAN to which the wireless station is assigned; and
- A class 4 that indicates access authorization to multiple access points included in a wide area network (WAN) (see fig. 4, ref. num 408A-D, 410A-B, and 412A-F of Watanabe et al.).

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Watanabe et al. (USPN '657).

Regarding claim 7, Watanabe et al. teaches all the limitations of claims 4 and 6, above. However, Watanabe et al. does not specifically teach wherein the second step of claim 6 further comprises the steps of: allocating a null encryption key if the determination result of the first step indicates that the access authorization does not correspond to said class 2; determining whether the access authorization corresponds to class 3; and allocating a null encryption key if a determination result indicates that the access authorization does not correspond to class 3.

Official Notice is taken that a null encryption key is allocated if the determining steps determines that the access authorization does not correspond to class 2 or 3.

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine allocating a null encryption key based on a determination that the access authorization does not correspond to class 2 or 3, with the method of Watanabe et al. It would have been obvious for such modifications because a null encryption key ensures that access is not obtained when access authorizations do not match. When a mobile device does not have authorization for a certain class, a null encryption key will prevent further access. If the null encryption key was not allocated to the mobile device, other data would be allocated and could possibly allow authorization.

### ***Response to Arguments***

8. Applicant argues: authentication is the process of identifying an individual requesting access to a system; it does not necessarily involve encryption and the cited passage of Watanabe is silent with respect to encryption (page 9 through page 11, first paragraph).

Regarding applicant's argument, examiner disagrees. Column 6, line 57 through column 7, line 16 and column 8, line 50 through column 9, line 22, further teaches that the authentication controller prepares pre-authentication and a shared key. The shared key is computed for each connection and is part of the pre-authentication process for establishment of a VPN between two networks.

***Conclusion***

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

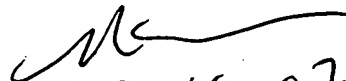
Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



BH

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
2,16,07